

# SUPERFAST SOLUTION OF TOEPLITZ SYSTEMS BASED ON SYZGY REDUCTION

HOUSAM KHALIL, BERNARD MOURRAIN, AND MICHELLE SCHATZMAN

**ABSTRACT.** We present a new superfast algorithm for solving Toeplitz systems. This algorithm is based on a relation between the solution of such problems and syzygies of polynomials or moving lines. We show an explicit connection between the generators of a Toeplitz matrix and the generators of the corresponding module of syzygies. We show that this module is generated by two elements and the solution of a Toeplitz system  $Tu = g$  can be reinterpreted as the remainder of a vector depending on  $g$ , by these two generators. We obtain these generators and this remainder with computational complexity  $\mathcal{O}(n \log^2 n)$  for a Toeplitz matrix of size  $n \times n$ .

## 1. INTRODUCTION

Structured matrices appear in various domains, such as scientific computing, signal processing, ... They usually express, in a linearize way, a problem which depends on fewer parameters than the number of entries of the corresponding matrix. An important area of research is devoted to the development of methods for the treatment of such matrices, which depend on the parameters defining them.

Among well-known structured matrices, Toeplitz and Hankel structures have been intensively studied [8, 12]. Nearly optimal algorithms are known for their multiplication by a vector and the solution of linear systems, for such structure. Namely, if  $A$  is a Toeplitz matrix of size  $n$ , multiplying it by a vector or solving a linear system with  $A$  requires  $\tilde{\mathcal{O}}(n)$  arithmetic operations (where  $\tilde{\mathcal{O}}(n) = \mathcal{O}(n \log^c(n))$  for some  $c > 0$ ) [2, 20]. Such algorithms are called superfast, in opposition with fast algorithms requiring  $\mathcal{O}(n^2)$  arithmetic operations.

The fundamental ingredients in these algorithms are the so-called generators [12], encoding the minimal information stored in these matrices, and on which the matrix transformations are translated. The correlation with other types of structured matrices has also been well developed in the literature [17, 16], allowing to treat efficiently other structures such as Vandermonde or Cauchy-like structures.

Such problems are strongly connected to polynomial problems [5, 1]. For instance, the product of a Toeplitz matrix by a vector can be deduced from the product of two univariate polynomials, and thus can be computed efficiently by evaluation-interpolation techniques, based on FFT. The inverse of a Hankel or Toeplitz matrix is connected to the Bezoutian of the polynomials associated to their generators. Such a construction is related to Gohberg-Semencul formula [7] (or Trench algorithm [18]), which describes the inverse of a Toeplitz matrix in terms of the solution of two specific Toeplitz systems (see also Gohberg-Prupnick formula [6]).

Most of these methods involve univariate polynomials. So far, few investigations have been pursued for the treatment of multilevel structured matrices [19, 13], related to multivariate problems. Such linear systems appear for instance in resultant or in residue constructions, in normal form computations, or more generally in multivariate polynomial algebra. We refer to [15] for a general description of multi-structured matrices and their correlations with multivariate polynomials. Surprisingly, these multivariate structure also appear in numerical scheme and preconditionners [13]. A main challenge here is to devise superfast algorithms of complexity  $\tilde{\mathcal{O}}(n)$  for the solution of multi-structured systems of size  $n$ .

In this paper, we re-investigate the solution of Toeplitz systems  $Tu = g$  from a new point of view which can be generalized to two-level Toeplitz systems. We correlate the solution of such problems with syzygies of polynomials. We show an explicit connection between the generators of a Toeplitz matrix and the generators of the corresponding module of syzygies. We show that this module is generated by two elements of degree  $n$  and the solution of  $Tu = g$  can be reinterpreted as the remainder of an explicit polynomial vector depending on  $g$ , by these two generators. We give two algorithms, with computational complexity  $\mathcal{O}(n \log^2 n)$ , to compute the generators of the module of syzygies. We give finally an algorithm, with computational complexity  $\mathcal{O}(n \log^2 n)$ , for the division of the generators

by the polynomial vector depending on  $g$ . Our new syzygy approach can be connected with Padé approximation method developed in [3] to compute efficiently particular solutions of Toeplitz linear system. But we replace the computation of generators of structured matrices by the computation of generators of a syzygy module and the solution of the linear system from particular solutions by Euclidean reduction by the generators of the syzygy module.

Let  $R = \mathbb{K}[x]$ . For  $n \in \mathbb{N}$ , we denote by  $\mathbb{K}[x]_n$  the vector space of polynomials of degree  $\leq n$ . Let  $L = \mathbb{K}[x, x^{-1}]$  be the set of Laurent polynomials in the variable  $x$ . For any polynomial  $p = \sum_{i=-m}^n p_i x^i \in L$ , we denote by  $p^+$  the sum of terms with non-negative exponents:  $p^+ = \sum_{i=0}^n p_i x^i$  and by  $p^-$ , the sum of terms with strictly negative exponents:  $p^- = \sum_{i=-m}^{-1} p_i x^i$ . We have  $p = p^+ + p^-$ .

For  $n \in \mathbb{N}$ , we denote by  $\mathfrak{U}_n = \{\omega; \omega^n = 1\}$  the set of roots of unity of order  $n$ .

For a vector  $u = (u_0, \dots, u_{k-1})^T \in \mathbb{K}^k$ , we denote by  $u(x)$  the polynomial of degree  $k-1$  given by  $u(x) = \sum_{i=0}^{k-1} u_i x^i$ . Conversely, if  $v(x) = \sum_{i=0}^{k-1} v_i x^i$  is a polynomial of degree  $k-1$ , we denote by  $v$  the vector of length  $k$  of coefficients of  $v(x)$ .

If no confusion arises, we may also use  $v$  to denote the polynomial  $v(x)$ .

## 2. SYZYGIES AND TOEPLITZ MATRICES

Let  $T \in \mathbb{K}^{n \times n}$  be an  $n \times n$  Toeplitz matrix. Then  $T$  is of the following form:

$$(1) \quad \begin{pmatrix} t_0 & t_{-1} & \dots & t_{-n+1} \\ t_1 & t_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & t_{-1} \\ t_{n-1} & \dots & t_1 & t_0 \end{pmatrix}.$$

Let  $g = (g_0, \dots, g_{n-1}) \in \mathbb{K}^n$  be a vector of length  $n$ . We are interested in the following problem:

**Problem 2.1.** Find  $u = (u_0, \dots, u_{n-1}) \in \mathbb{K}^n$  such that

$$(2) \quad Tu = g.$$

**Definition 2.2.** Let  $E = \{1, \dots, x^{n-1}\}$ , and  $\Pi_E$  be the projection of  $L$  on the vector space generated by  $E$ , along  $\langle x^n, x^{n+1}, \dots \rangle$ .

**Definition 2.3.** From the matrix  $T$  and the vectors  $g$  and  $u$  we define the following polynomials:

- $T(x) = \sum_{i=-n+1}^{n-1} t_i x^i,$
- $\tilde{T}(x) = \sum_{i=0}^{2n-1} \tilde{t}_i x^i$  with  $\tilde{t}_i = \begin{cases} t_i & \text{if } i < n \\ t_{i-2n} & \text{if } i \geq n \end{cases},$
- $u(x) = \sum_{i=0}^{n-1} u_i x^i, g(x) = \sum_{i=0}^{n-1} g_i x^i.$

Notice that  $T(x)$  is a Laurent polynomial and that  $\tilde{T}(x)$  is a polynomial of degree  $2n-1$ . By construction, we have the following properties:

**Proposition 2.4.**  $\tilde{T} = T^+ + x^{2n} T^-$  and  $T(w) = \tilde{T}(w)$  if  $w \in \mathfrak{U}_{2n}$ .

*Proof.* We can deduce directly, from the definition of  $T(x)$  and  $\tilde{T}(x)$ , that  $\tilde{T} = T^+ + x^{2n} T^-$ . Moreover, since  $w^{2n} = 1$  and  $\tilde{T}(x) = T^+(x) + x^{2n} T^-(x)$ , then  $\tilde{T}(w) = T^+(w) + T^-(w) = T(w)$ .  $\square$

According to Proposition 2.1.2 of [15], we have the following relation between the problem 2.1 and polynomials:

**Proposition 2.5.** We have

$$Tu = g \Leftrightarrow \Pi_E(T(x)u(x)) = g(x).$$

As  $\Pi_E(T(x)u(x))$  is the polynomial  $T(x)u(x)$  from which we remove terms of negative degree and of degree  $\geq n$ , then we can write  $T(x)u(x)$  as following:

**Proposition 2.6.**

$$(3) \quad T(x)u(x) = \Pi_E(T(x)u(x)) + x^{-n}A(x) + x^n B(x),$$

where  $A(x) \in \mathbb{K}[x]_{n-1}$  and  $B(x) \in \mathbb{K}[x]_{n-2}$ .

*Proof.* By expanding  $T(x)u(x)$  we can write

$$\begin{aligned} T(x)u(x) &= \Pi_E(T(x)u(x)) + (\alpha_{-n+1}x^{-n+1} + \cdots + \alpha_{-1}x^{-1}) + (\alpha_n x^n + \cdots + \alpha_{2n-2}x^{2n-2}) \\ &= \Pi_E(T(x)u(x)) + x^{-n}(\alpha_{-n+1}x + \cdots + \alpha_{-1}x^{n-1}) + x^n(\alpha_n + \cdots + \alpha_{2n-2}x^{n-2}) \\ &= \Pi_E(T(x)u(x)) + x^{-n}A(x) + x^nB(x) \end{aligned}$$

□

Therefore, according to Proposition 2.5 and Proposition 2.6, if  $u$  is solution of  $Tu = g$  then there exist two polynomials  $A(x)$  and  $B(x)$  in  $\mathbb{K}[x]_{n-1}$  such that

$$(4) \quad T(x)u(x) - x^{-n}A(x) - x^nB(x) = g(x).$$

By evaluation at the roots  $\omega \in \mathfrak{U}_{2n}$ , and since  $\omega^{-n} = \omega^n$  and  $\tilde{T}(\omega) = T(\omega)$  for  $\omega \in \mathfrak{U}_{2n}$ , we have

$$\tilde{T}(\omega)u(\omega) + \omega^n v(\omega) = g(\omega), \forall \omega \in \mathfrak{U}_{2n}(\omega),$$

where  $v(x) = -A(x) - B(x)$  of degree  $\leq n-1$ . Therefore the polynomial  $\tilde{T}(x)u(x) + x^n v(x) - g(x)$  is multiple of  $x^{2n} - 1$ . We deduce that there exists  $w(x) \in \mathbb{K}[x]$  such that

$$(5) \quad \tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = g(x).$$

Notice that  $w(x)$  is of degree  $\leq n-1$  because  $(x^{2n} - 1)w(x)$  is of degree  $\leq 3n-1$ .

**2.1. Syzygies.** The solutions of Equation (5) is a particular case of the following problem, related to interesting questions in Effective Algebraic Geometry.

**Problem 2.7.** *Given three polynomials  $a, b, c \in R$  respectively of degree  $< l, < m, < n$ , find three polynomials  $p, q, r \in R$  of degree  $< \nu - l, < \nu - m, < \nu - n$ , such that*

$$(6) \quad a(x)p(x) + b(x)q(x) + c(x)r(x) = 0.$$

The polynomial vector  $(p, q, r) \in \mathbb{K}[x]^3$  is called a *syzygy* of  $(a, b, c)$ . We denote by  $\mathcal{L}(a, b, c)$  the set of syzygies  $(p, q, r) \in \mathbb{K}[x]^3$  of  $(a, b, c)$ , i.e. the solutions of (6). It is a  $\mathbb{K}[x]$ -module of  $\mathbb{K}[x]^3$  and it is called the module of syzygies of  $(a, b, c)$ . The solutions of Problem 2.7 are  $\mathcal{L}(a, b, c) \cap \mathbb{K}[x]_{\nu-l-1} \times \mathbb{K}[x]_{\nu-m-1} \times \mathbb{K}[x]_{\nu-n-1}$ .

Given a new polynomial  $d(x) \in \mathbb{K}[x]$ , we denote by  $\mathcal{L}(a, b, c; d)$  the set of  $(p, q, r) \in \mathbb{K}[x]^3$  such that

$$(7) \quad a(x)p(x) + b(x)q(x) + c(x)r(x) = d(x).$$

**Theorem 2.8.** *For any non-zero vector of polynomials  $(a, b, c) \in \mathbb{K}[x]^3$ , the  $\mathbb{K}[x]$ -module  $\mathcal{L}(a, b, c)$  is free of rank 2.*

*Proof.* By the Hilbert's theorem, the ideal  $I$  generated by  $(a, b, c)$  has a free resolution of length at most 1 (see [4, chap. 6]), that is of the form:

$$0 \rightarrow \mathbb{K}[x]^p \rightarrow \mathbb{K}[x]^3 \rightarrow \mathbb{K}[x] \rightarrow \mathbb{K}[x]/I \rightarrow 0.$$

As  $I \neq 0$ , for dimensional reasons, we must have  $p - 3 + 1 = 0$ , then  $p = 2$ . □

**Definition 2.9.** *For a polynomial vector  $p = (p_1, \dots, p_k) \in \mathbb{K}[x]^k$ , we define*

$$\deg(p_1, \dots, p_k) = \max(\deg(p_1), \dots, \deg(p_k)).$$

**Definition 2.10.** *Assume that  $\deg(p, q, r) \leq \deg(p', q', r')$ . A  $\mu$ -base of  $\mathcal{L}(a, b, c)$  is a basis  $\{(p, q, r), (p', q', r')\}$  of  $\mathcal{L}(a, b, c)$ , with  $\deg(p, q, r) = \mu$ .*

We have the following relation between the degrees of the two elements of a basis of  $\mathcal{L}(a, b, c)$ :

**Proposition 2.11.** *Let  $\{(p_1, q_1, r_1), (p_2, q_2, r_2)\}$  be a basis of  $\mathcal{L}(a, b, c)$ ,  $\mu_1 = \deg(p_1, q_1, r_1)$  and  $\mu_2 = \deg(p_2, q_2, r_2)$ . We have  $\deg(a, b, c) = \mu_1 + \mu_2$ .*

*Proof.* We have

$$0 \rightarrow \mathbb{K}[x]_{\nu-d-\mu_1} \oplus \mathbb{K}[x]_{\nu-d-\mu_2} \rightarrow \mathbb{K}[x]_{\nu-d}^3 \rightarrow \mathbb{K}[x]_{\nu} \rightarrow \mathbb{K}[x]_{\nu}/(a, b, c)_{\nu} \rightarrow 0,$$

for  $\nu \gg 0$ . As the alternate sum of the dimension of the  $\mathbb{K}$ -vector spaces is zero and  $\mathbb{K}[x]_{\nu}/(a, b, c)_{\nu}$  is 0 for  $\nu \gg 0$ , we have

$$0 = 3(d - \nu - 1) + \nu - \mu_1 - d + 1 + \nu - \mu_2 - d + 1 + \nu + 1 = d - \mu_1 - \mu_2.$$

□

**2.2. The module  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ .** Returning to the initial problem, we saw that if  $u$  is solution of  $Tu = g$  then there exist two polynomials  $v(x)$  and  $w(x)$  in  $\mathbb{K}[x]_{n-1}$  such that  $(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x))$ .

By the proposition 2.11, if  $(p, q, r)$  and  $(p', q', r')$  form a basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  of degree  $\mu_1$  and  $\mu_2$  respectively then we have  $\mu_1 + \mu_2 = 2n$ . We are going to show now that in fact  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  has a  $n$ -basis, that is a basis of two elements of degree  $\mu_1 = \mu_2 = n$ :

**Proposition 2.12.** *The  $\mathbb{K}[x]$ -module  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  has a  $n$ -basis.*

*Proof.* Consider the linear map  $\mathbb{K}[x]_{n-1}^3 \rightarrow \mathbb{K}[x]_{3n-1}$

$$(p(x), q(x), r(x)) \mapsto \tilde{T}(x)p(x) + x^n q(x) + (x^{2n} - 1)r(x),$$

which  $3n \times 3n$  matrix is of the form

$$(9) \quad S := \left( \begin{array}{c|c|c} T_0 & \mathbf{0} & -\mathbb{I}_n \\ T_1 & \mathbb{I}_n & \mathbf{0} \\ T_2 & \mathbf{0} & \mathbb{I}_n \end{array} \right),$$

where  $T_0, T_1, T_2$  are the coefficient matrices of  $(\tilde{T}(x), x\tilde{T}(x), \dots, x^n\tilde{T}(x))$ , respectively for the list of monomials  $(1, \dots, x^{n-1})$ ,  $(x^n, \dots, x^{2n-1})$ ,  $(x^{2n}, \dots, x^{3n-1})$ . Notice in particular that  $T = T_0 + T_2$ .

Reducing the first block  $(T_0|\mathbf{0}|-\mathbb{I}_n)$  by the last block  $(T_2|\mathbf{0}|\mathbb{I}_n)$ , we replace it by the block  $(T_0 + T_2|\mathbf{0}|\mathbf{0})$ , without changing the rank of  $S$ . As  $T = T_0 + T_2$  is invertible, this shows that the matrix  $S$  is of rank  $3n$ . Therefore  $\ker(S) = 0$  and there is no syzygies in degree  $n - 1$ .

As the sum  $2n = \mu_1 + \mu_2$ , where  $\mu_1, \mu_2$  are the degrees of a pair of generators of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ , and as  $\mu_1 \geq n$  and  $\mu_2 \geq n$ , we have  $\mu_1 = \mu_2 = n$ . Moreover,  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  is free of rank 2. Thus there exist two linearly independent syzygies  $(u_1, v_1, w_1)$ ,  $(u_2, v_2, w_2)$  of degree  $n$ , which generate  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ .  $\square$

A similar result can also be found in [20], but the proof much longer than this one, is based on interpolation techniques and explicit computations.

Let us now describe how to construct explicitly two generators  $(u_1, v_1, w_1)$ ,  $(u_2, v_2, w_2)$  of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  of degree  $n$ . As  $\tilde{T}(x)$  is of degree  $\leq 2n - 1$  and the map (8) is surjective, there exists  $(u, v, w) \in \mathbb{K}[x]_{n-1}^3$  such that

$$(10) \quad \tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w = \tilde{T}(x)x^n.$$

We deduce that  $(u_1, v_1, w_1) = (x^n - u, -v, -w) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ .

Since there exists  $(u', v', w') \in \mathbb{K}[x]_{n-1}^3$  such that

$$(11) \quad \tilde{T}(x)u'(x) + x^n v'(x) + (x^{2n} - 1)w' = 1 = x^n x^n - (x^{2n} - 1),$$

we deduce that  $(u_2, v_2, w_2) = (-u', x^n - v', -w' - 1) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ .

Now,  $T$  and  $\tilde{T}$  are linearly independent since by construction, The coefficient vectors of  $x^n$  in  $(u_1, v_1, w_1)$  and  $(u_2, v_2, w_2)$  are respectively  $(1, 0, 0)$  and  $(0, 1, 0)$ , which shows that vectors  $(u_1, v_1, w_1)$ ,  $(u_2, v_2, w_2) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1) \cap \mathbb{K}[x]_n$  are linearly independent. Therefore, they form a basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ .

Now we can prove our aim theorem:

**Theorem 2.13.** *The vector  $u$  is solution of (2) if and only if there exist  $v(x)$  and  $w(x)$  in  $\mathbb{K}[x]_{n-1}$  such that*

$$(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x))$$

*Proof.* If  $u$  is solution of (2), we see that there exist  $v(x) \in \mathbb{K}[x]_{n-1}$  and  $w(x) \in \mathbb{K}[x]_{n-1}$  such that

$$\tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = g(x).$$

Conversely, a solution  $(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}[x]_{n-1}^3$  implies that  $(u, v, w) \in \mathbb{K}^{3n}$  is a solution of the linear system:

$$S \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} g \\ 0 \\ 0 \end{pmatrix},$$

where  $S$  is has the block structure (9), so that  $T_2 u + w = 0$  and  $T_0 u - w = (T_0 + T_2)u = g$ . As we have  $T_0 + T_2 = T$ , the vector  $u$  is a solution of (2), which ends the proof of the theorem.  $\square$

Computing the inverse of a Toeplitz matrix  $T$  is equivalent to computing the first and the last column of  $T^{-1}$ , based on Gohberg-Semencul decomposition (see [9, 14, 10, 11] for more details about Gohberg-Semencul decomposition).

We are going to show that the solutions of Equations (10) and (11) which gives us the  $n$ -basis  $\{(u_1, v_1, w_1), (u_2, v_2, w_2)\}$  is related to the solution of two specific Toeplitz linear systems.

**Proposition 2.14.** *Let  $(u(x), v(x), w(x))$  and  $(u'(x), v'(x), w'(x))$  be in  $\mathbb{K}_{n-1}[x]^3$  such that*

$$\begin{cases} \tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = \tilde{T}(x)x^n, \\ \tilde{T}(x)u'(x) + x^n v'(x) + (x^{2n} - 1)w'(x) = 1. \end{cases}$$

*Then  $Tu' = e_1$  and  $Tu = ZTe_n$ , with  $Z$  is the lower shift matrix of size  $n$ .*

*Proof.* As  $u'(x)$ ,  $v'(x)$ ,  $w'(x)$  and 1 are of degree  $\leq n-1$ , then, by Theorem 2.13,  $\tilde{T}(x)u'(x) + x^n v'(x) + (x^{2n} - 1)w'(x) = 1$  is equivalent to  $Tu' = e_1$  ( $e_1(x) = 1$ ) and  $u'$  is the first column of  $T^{-1}$ .

We have  $\tilde{T}(x) = T_+(x) + x^{2n}T_-(x)$ , then

$$\tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = x^n T_+(x) + x^n((x^{2n} - 1)T_-(x) + T_-(x)).$$

Therefore,

$$\tilde{T}(x)u(x) + x^n(v(x) - T_+(x)) + (x^{2n} - 1)(w(x) - x^n T_-(x)) = x^n T_-(x).$$

As  $x^n T_-(x)$  is of degree  $\leq n-1$  and is the polynomial associated with the vector  $ZTe_n$ , by Theorem 2.13,  $u$  is such that  $Tu = ZTe_n$ .  $\square$

Notice that  $u$  is not the last column of  $T^{-1}$ , but we can use  $u$  and  $u'$  to compute it (see [9]). Therefore, defining a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  from the solution of Equations (10) and (11) is equivalent to computing the Gohberg-Semencul decomposition of  $T^{-1}$ .

In the following section, we reduce translation of the solution of  $Tu = g$  to an Euclidean division, based on our decomposition, instead of multiplying  $g$  by triangular Toeplitz matrices, based on Gohberg-Semencul decomposition. The advantage of our decomposition is that we can generalized it to two-level problems, which allows us to describe a ‘‘Gohberg-Semencul’’ decomposition of Toeplitz-block-Toeplitz matrices.

### 3. EUCLIDEAN DIVISION

In this section, we show how to obtain the solution vector  $(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}[x]_n^3$  from a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  and a particular solution in  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x))$ .

From Theorem 2.13 we deduce the two following corollaries:

**Corollary 3.1.** *For all  $g(x) \in \mathbb{K}_{n-1}[x]$ , the set  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}_{n-1}^3[x]$  has exactly one element.*

*Proof.* As  $T$  is invertible, there exists a unique  $u$  such that  $Tu = g$ . From the theorem 2.13, there exists  $v(x)$ ,  $w(x)$  of degree  $\leq n-1$ , such that  $(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}_{n-1}^3[x]$ .

The uniqueness is also obvious: if  $(u'(x), v'(x), w'(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}_{n-1}^3[x]$ , then  $(u(x), v(x), w(x)) - (u'(x), v'(x), w'(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1) \cap \mathbb{K}_{n-1}^3[x]$  which equal  $\{(0, 0, 0)\}$  (see the demonstration of the proposition 2.12). Then  $(u(x), v(x), w(x)) = (u'(x), v'(x), w'(x))$ .  $\square$

**Corollary 3.2.** *Let  $\{(u_1, v_1, w_1), (u_2, v_2, w_2)\}$  be a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ . Let  $(p, q, r)$  be in  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x))$ . There exists a unique  $(u, v, w) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}_{n-1}^3[x]$  and a unique pair of polynomials  $p_1$  and  $p_2$  such that*

$$\begin{pmatrix} p \\ q \\ r \end{pmatrix} = p_1 \begin{pmatrix} u_1 \\ v_1 \\ w_1 \end{pmatrix} + p_2 \begin{pmatrix} u_2 \\ v_2 \\ w_2 \end{pmatrix} + \begin{pmatrix} u \\ v \\ w \end{pmatrix}.$$

*This decomposition is called the division of  $(p, q, r)$  by  $(u_1, v_1, w_1)$  and  $(u_2, v_2, w_2)$ .*

*Proof.* From the previous corollary, there exist a unique element in  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}_{n-1}^3[x]$ , let  $(u, v, w)$  be this element. As  $\{(u_1, v_1, w_1), (u_2, v_2, w_2)\}$  is a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ , and as

$(p, q, r) - (u, v, w) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ , then there exist a unique pair of polynomials unique  $p_1$  and  $p_2$  such that

$$\begin{pmatrix} p \\ q \\ r \end{pmatrix} - \begin{pmatrix} u \\ v \\ w \end{pmatrix} = p_1 \begin{pmatrix} u_1 \\ v_1 \\ w_1 \end{pmatrix} + p_2 \begin{pmatrix} u_2 \\ v_2 \\ w_2 \end{pmatrix}$$

□

As a consequence of the two corollaries, we have the following important property:

**Theorem 3.3.** *Let  $\{(u_1, v_1, w_1), (u_2, v_2, w_2)\}$  be a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ , and let  $g \in \mathbb{K}^n$ . The remainder of the division of  $\begin{pmatrix} 0 \\ x^n g \\ g \end{pmatrix}$  by  $\begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \\ w_1 & w_2 \end{pmatrix}$  is the unique element  $(u, v, w) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}_{n-1}^3[x]$ , and therefore  $u$  is the solution of  $Tu = g$ .*

*Proof.* The vector  $\begin{pmatrix} 0 \\ x^n g \\ -g \end{pmatrix} \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g)$  is a particular solution. We reduce it by  $\begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \\ w_1 & w_2 \end{pmatrix}$  and obtain

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ x^n g \\ g \end{pmatrix} - \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \\ w_1 & w_2 \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix},$$

where  $(u, v, w) \in \mathbb{K}[x]_{n-1}^3 \cap \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g)$  is the remainder of division. Thus  $(u, v, w)$  is the unique vector  $\in \mathbb{K}[x]_{n-1}^3 \cap \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g)$ . □

A way to perform the division is to choose a  $n$ -basis  $\{(u_1, v_1, w_1), (u_2, v_2, w_2)\}$  of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  so that the  $2 \times 2$  coefficient matrix of  $x^n$  in

$$\begin{pmatrix} u_1(x) & u_2(x) \\ v_1(x) & v_2(x) \end{pmatrix}$$

is invertible. In this case we can reduce the polynomial  $(0, x^n g(x))$  to reach to a degree  $< n - 1$  and we can write in a unique way

$$\begin{pmatrix} 0 \\ x^n g(x) \end{pmatrix} = p_1 \begin{pmatrix} u_1 \\ v_1 \end{pmatrix} + p_2 \begin{pmatrix} u_2 \\ v_2 \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix}.$$

By the uniqueness of the remainder in the Euclidean division, we obtain the following proposition:

**Proposition 3.4.** *The first coordinate of the remainder in the division of  $\begin{pmatrix} 0 \\ x^n g \end{pmatrix}$  by  $\begin{pmatrix} u & u_2 \\ v_1 & v_2 \end{pmatrix}$  is the polynomial  $u(x)$  such that its associated vector  $u$  is the solution of  $Tu = g$ .*

So we set the following problem:

**Problem 3.5.** *Given a matrix and a vector of polynomials  $\begin{pmatrix} e(x) & e'(x) \\ f(x) & f'(x) \end{pmatrix}$  of degree  $n$  such that  $\begin{pmatrix} e_n & e'_n \\ f_n & f'_n \end{pmatrix}$  is invertible and  $\begin{pmatrix} p(x) \\ q(x) \end{pmatrix}$  of degree  $m \geq n$ , find the remainder of the division of  $\begin{pmatrix} p(x) \\ q(x) \end{pmatrix}$  by  $\begin{pmatrix} e(x) & e'(x) \\ f(x) & f'(x) \end{pmatrix}$ .*

We describe here a generalized Euclidean division algorithm to solve problem 3.5.

Let  $E(x) = \begin{pmatrix} p(x) \\ q(x) \end{pmatrix}$  of degree  $m$ ,  $B(x) = \begin{pmatrix} e(x) & e'(x) \\ f(x) & f'(x) \end{pmatrix}$  of degree  $n \leq m$ .  $E(x) = B(x)Q(x) + R(x)$  with  $\deg(R(x)) < n$ , and  $\deg(Q(x)) \leq m - n$ . Let  $z = \frac{1}{x}$ . We have

$$\begin{aligned}
 E(x) &= B(x)Q(x) + R(x) \\
 \Leftrightarrow E\left(\frac{1}{z}\right) &= B\left(\frac{1}{z}\right)Q\left(\frac{1}{z}\right) + R\left(\frac{1}{z}\right) \\
 \Leftrightarrow z^m E\left(\frac{1}{z}\right) &= z^n B\left(\frac{1}{z}\right)z^{m-n}Q\left(\frac{1}{z}\right) + z^{m-n+1}z^{n-1}R\left(\frac{1}{z}\right) \\
 (12) \quad \Leftrightarrow \hat{E}(z) &= \hat{B}(z)\hat{Q}(z) + z^{m-n+1}\hat{R}(z)
 \end{aligned}$$

with  $\hat{E}(z), \hat{B}(z), \hat{Q}(z), \hat{R}(z)$  are the polynomials obtained by reversing the order of coefficients of polynomials  $E(z), B(z), Q(z), R(z)$ .

$$\begin{aligned}
 (12) \quad \Rightarrow \hat{B}(z)^{-1}\hat{E}(z) &= \hat{Q}(z) + z^{m+n-1}\hat{B}(z)^{-1}\hat{R}(z) \\
 \Rightarrow \hat{Q}(z) &= \hat{B}(z)^{-1}\hat{E}(z) \pmod{z^{m-n+1}}
 \end{aligned}$$

The formal power series  $\hat{B}(z)^{-1}$  exists because the constant coefficient of  $\hat{B}(z)$  is invertible. Thus  $\hat{Q}(z)$  is obtained by computing the first  $m - n + 1$  coefficients of  $\hat{B}(z)^{-1}\hat{E}(z)$ , which is obtained by computing  $W(x) = \hat{B}(z)^{-1}$ , then by multiplying  $W(x)$  by  $\hat{E}(z)$ .

To find  $W(x) = \hat{B}(z)^{-1}$  we use Newton's iteration. Let  $f(W) = \hat{B} - W^{-1}$ . We have

$$f'(W_l) \cdot (W_{l+1} - W_l) = -W_l^{-1}(W_{l+1} - W_l)W_l^{-1} = f(W_l) = \hat{B} - W_l^{-1}.$$

Thus we set

$$W_{l+1} = 2W_l - W_l \hat{B} W_l,$$

and  $W_0 = \hat{B}_0^{-1}$ , which exists. Moreover, we have

$$\begin{aligned}
 W - W_{l+1} &= W - 2W_l + W_l \hat{B} W_l \\
 &= W(\mathbb{I}_2 - \hat{B} W_l)^2 \\
 &= (W - W_l) \hat{B} (W - W_l)
 \end{aligned}$$

Thus  $W_l(x) = W(x) \pmod{x^{2l}}$  for  $l = 0, \dots, \lceil \log(m - n + 1) \rceil$ .

**Proposition 3.6.** *We need  $\mathcal{O}(n \log(n) \log(m - n) + m \log m)$  operations to solve problem 3.5.*

*Proof.* We must do  $\lceil \log(m - n + 1) \rceil$  Newton's iteration to obtain the first  $m - n + 1$  coefficients of  $\hat{B}(z)^{-1} = W(x)$ . And each iteration requires  $\mathcal{O}(n \log n)$  operations (multiplication and summation of polynomials of degree  $n$ ). Finally, multiplication  $\hat{B}(z)^{-1}\hat{E}(z)$  requires  $\mathcal{O}(m \log m)$  operations.  $\square$

Notice that, for our problem  $m = n$  and this algorithm requires  $\mathcal{O}(n \log^2 n)$  arithmetic operations. In the following section, we show how to compute a  $n$ -basis in  $\mathcal{O}(n \log^2 n)$  arithmetic operations.

#### 4. CONSTRUCTION OF THE GENERATORS

The canonical basis of  $\mathbb{K}[x]^3$  is denoted by  $\sigma_1, \sigma_2, \sigma_3$ . Let  $\rho_1, \rho_2$  be the generators of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  of degree  $n$  given by

$$\begin{aligned}
 (13) \quad \rho_1 &= x^n \sigma_1 - (u, v, w) = (u_1, v_1, w_1) \\
 \rho_2 &= x^n \sigma_2 - (u', v', w') = (u_2, v_2, w_2),
 \end{aligned}$$

where  $(u, v, w), (u', v', w')$  are the vectors given in (10) and (11).

We describe two methods for computing  $(u_1, v_1, w_1)$  and  $(u_2, v_2, w_2)$ . The first one uses the Euclidean gcd algorithm, the second one is based on the method in [20].

We recall firstly the algebraic and computational properties of the well known extended euclidean algorithm (see [21]): Given  $p(x), p'(x)$  two polynomials in degree  $m$  and  $m'$  respectively, let

$$\begin{aligned}
 r_0 &= p, & r_1 &= p', \\
 s_0 &= 1, & s_1 &= 0, \\
 t_0 &= 0, & t_1 &= 1.
 \end{aligned}$$

and define

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i, \\ s_{i+1} &= s_{i-1} - q_i s_i, \\ t_{i+1} &= t_{i-1} - q_i t_i, \end{aligned}$$

where  $q_i$  results when the division algorithm is applied to  $r_{i-1}$  and  $r_i$ , i.e.  $r_{i-1} = q_i r_i + r_{i+1}$ .

**Proposition 4.1.** *Let  $l \in \mathbb{N}$  such that  $r_l = 0$ . Then  $r_{l-1} = \gcd(p(x), p'(x))$ .*

And more generally we have:

**Proposition 4.2.** *For all  $i = 1, \dots, l$  we have*

$$s_i p + t_i p' = r_i \quad \text{and} \quad (s_i, t_i) = 1,$$

and

$$\begin{cases} \deg r_{i+1} < \deg r_i, & i = 1, \dots, l-1 \\ \deg s_{i+1} > \deg s_i & \text{and} \quad \deg t_{i+1} > \deg t_i, \\ \deg s_{i+1} = \deg(q_i \cdot s_i) = \deg v - \deg r_i, \\ \deg t_{i+1} = \deg(q_i \cdot t_i) = \deg u - \deg r_i. \end{cases}$$

We can now present our algorithm. It can be found in the proof of the following theorem:

**Theorem 4.3.** *By applying the Euclidean gcd algorithm to  $p(x) = x^{n-1}T$  and  $p'(x) = x^{2n-1}$  stopping in degree  $n-1$  and  $n-2$ , we obtain  $\rho_1$  and  $\rho_2$  respectively.*

*Proof.* We see that  $Tu = g$  if and only if there exist  $a(x)$  and  $b(x)$  in  $\mathbb{K}[x]_{n-1}$  such that

$$\bar{T}(x)u(x) + x^{2n-1}b(x) = x^{n-1}g(x) + a(x),$$

where  $\bar{T}(x) = x^{n-1}T(x)$  is a polynomial of degree  $\leq 2n-2$ . In (10) and (11) we saw that for  $g(x) = 1$  ( $g = e_1$ ) and  $g(x) = x^n T(x)$  ( $g = (0, t_{-n+1}, \dots, t_{-1})^T$ ) we obtain a base of  $\mathcal{L}(\bar{T}(x), x^n, x^{2n-1})$ .

Notice that  $Tu_1 = e_1$  if and only if there exist  $a_1(x) \in \mathbb{K}[x]_{n-2}$ ,  $b_1(x) \in \mathbb{K}[x]_{n-1}$  such that

$$(14) \quad \bar{T}(x)u_1(x) + x^{2n-1}b_1(x) = x^{n-1} + a_1(x),$$

and  $Tu_2 = (0, t_{-n+1}, \dots, t_{-1})^T$  if and only if there exist  $a_2(x) \in \mathbb{K}[x]_{n-2}$ ,  $b_2(x) \in \mathbb{K}[x]_{n-1}$  such that

$$(15) \quad \bar{T}(x)(u_2(x) + x^n) + x^{2n-1}b_2(x) = a_2(x).$$

As  $\deg a_1(x) \leq n-2$  and  $\deg a_2(x) \leq n-2$ , by applying the extended Euclidean algorithm in  $p(x) = x^{n-1}T$  and  $p'(x) = x^{2n-1}$  until we have  $\deg r_l(x) = n-1$  and  $\deg r_{l+1}(x) = n-2$  we obtain

$$u_1(x) = \frac{1}{c_1}s_l(x), \quad b_1(x) = \frac{1}{c_1}t_l(x), \quad x^{n-1} + a_1(x) = \frac{1}{c_1}r_l(x),$$

and

$$x^n + u_2(x) = \frac{1}{c_2}s_{l+1}(x), \quad b_2(x) = \frac{1}{c_2}t_{l+1}(x), \quad a_2(x) = \frac{1}{c_2}r_{l+1}(x),$$

with  $c_1$  and  $c_2$  are the highest coefficients of  $r_l(x)$  and  $s_{l+1}(x)$  respectively. In fact, Equation (14) is equivalent to

$$\begin{array}{c} n-1 \\ \left\{ \begin{array}{c} \overbrace{\begin{pmatrix} t_{-n+1} & & \\ \vdots & \ddots & \\ t_0 & \dots & t_{-n+1} \end{pmatrix}}^n \\ \overbrace{\begin{pmatrix} \vdots & \ddots & \vdots \\ t_{n-1} & \dots & t_0 \end{pmatrix}}^{n-1} \\ \vdots \\ \begin{pmatrix} & & \\ & \ddots & \\ & & t_{n-1} \end{pmatrix} \end{array} \right\} \begin{array}{c} \overbrace{\begin{pmatrix} & & \\ & & \\ & & 1 \end{pmatrix}}^{n-1} \\ \vdots \\ \begin{pmatrix} & & \\ & \ddots & \\ & & 1 \end{pmatrix} \end{array} \end{array} \begin{pmatrix} u_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

since  $T$  is invertible then the  $(2n-1) \times (2n-1)$  block at the bottom is invertible and then  $u_1$  and  $b_1$  are unique. Therefore  $a_1$  is also unique.



As  $\deg r_l = n - 1$  then, by Proposition 4.2,  $\deg s_{l+1} = (2n - 1) - (n - 1) = n$  and  $\deg t_{l+1} = (2n - 2) - (n - 1) = n - 1$ . By the same proposition, we also have  $\deg s_l \leq n - 1$  and  $\deg t_l \leq n - 2$ .

Therefore,  $\deg u_1 = \deg s_l$  and  $\deg b_1 = \deg t_l$ . Then as  $u_1(x)$  and  $\frac{1}{c_1}s_l$  are unitaries,  $\frac{1}{c_1}s_l(x) = u_1(x)$  which implies that  $\frac{1}{c_1}t_l(x) = b_1(x)$ . For the same reasons, we have  $x^n + u_2(x) = \frac{1}{c_2}s_{l+1}(x)$  and  $b_2(x) = \frac{1}{c_2}t_{l+1}(x)$ .

Finally,  $Tu = e_1$  if and only if there exist  $v(x)$ ,  $w(x)$  such that

$$(16) \quad \tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = 1.$$

As  $\tilde{T}(x) = T^+ + x^{2n}T^- = T + (x^{2n} - 1)T^-$ , we deduce that

$$(17) \quad T(x)u(x) + x^n v(x) + (x^{2n} - 1)(w(x) + T^-(x)u(x)) = 1.$$

Moreover, we also have  $T(x)u(x) - x^{-n+1}a_1(x) + x^n b_1(x) = 1$  and  $x^{-n+1}a_1(x) = x^n(x a_1) - x^{-n}(x^{2n} - 1)x a_1$ . Thus

$$(18) \quad T(x)u(x) + x^n(b(x) - x a(x)) + (x^{2n} - 1)x^{-n+1}a(x) = 1.$$

Comparing (17) and (18), and as  $1 = x^n x^n - (x^{2n} - 1)$  we deduce that  $w(x) = x^{-n+1}a(x) - T^-(x)u(x) + 1$ , which is the part of positive degree of  $-T^-(x)u(x) + 1$ . This conclude the proof of the proposition.  $\square$

**Remark 4.4.** *The usual Euclidean gcd algorithms are of computational complexity  $\mathcal{O}(n^2)$ , but superfast euclidean gcd algorithms use no more then  $\mathcal{O}(n \log^2 n)$  operations, exist. See for example [21] chapter 11.*

The second method for computing  $(u_1, v_1, w_1)$  and  $(u_2, v_2, w_2)$  is of polynomials and interpolation points. We are interested in computing the coefficients of the canonical basis element  $\sigma_1, \sigma_2$  in this basis. The coefficients of  $\sigma_3$  can be obtained by reduction of  $(\tilde{T}(x)x^n)B(x)$  by  $x^{2n} - 1$  where

$$B(x) = \begin{pmatrix} u(x) & u'(x) \\ v(x) & v'(x) \end{pmatrix},$$

where  $(u, v)$ ,  $(u', v')$  are the two first coordinates of the solution of Equations (10) and (11). A superfast algorithm for computing  $B(x)$  is given in [20]. Let us describe how to compute it.

By evaluation of (13) at the roots  $\omega_j \in \mathfrak{U}_{2n}$ , we deduce that  $(u(x), v(x))$  and  $(u'(x), v'(x))$  are the solution of the following rational interpolation problem:

$$\begin{cases} \tilde{T}(\omega_j)u(\omega_j) + \omega_j^n v(\omega_j) = 0 \\ \tilde{T}(\omega_j)u'(\omega_j) + \omega_j^n v'(\omega_j) = 0 \end{cases},$$

with

$$\begin{cases} u_n = 1, v_n = 0, \\ u'_n = 0, v'_n = 1. \end{cases}$$

**Definition 4.5.** *The  $\tau$ -degree of a vector polynomial  $w(x) = (w_1(x) w_2(x))^T$  is defined as*

$$\tau - \deg w(x) := \max\{\deg w_1(x), \deg w_2(x) - \tau\}$$

**Definition 4.6.** *A polynomial vector in  $\mathbb{K}[x]^2$  is called  $\tau$ -reduced if the  $\tau$ -highest degree coefficients are linearly independent.*

By construction, the columns of  $B(x)$  form a  $n$ -reduced basis of the module of polynomial vectors  $r(x) \in \mathbb{K}[x]^2$  that satisfy the interpolation conditions

$$f_j r(\omega_j) = 0, \quad j = 0, \dots, 2n - 1$$

with  $f_j = (\tilde{T}(\omega_j), \omega_j^n) \in \mathbb{K}^2$ . The columns of  $B(x)$  are also called a  $n$ -reduced basis for the interpolation data  $(\omega_j, f_j)$ ,  $j = 0, \dots, 2n - 1$ .

**Theorem 4.7.** *Let  $\tau = n$  and  $J$  be a positive integer. Let  $\lambda_1, \dots, \lambda_J \in \mathbb{K}$  and  $\phi_1, \dots, \phi_J \in \mathbb{K}^2 \setminus \{(0, 0)\}$ . Let  $1 \leq j \leq J$  and  $\tau_j \in \mathbb{Z}$ . Suppose that  $B_j(x) \in \mathbb{K}[x]^{2 \times 2}$  is a  $\tau_j$ -reduced basis matrix with basis vectors having  $\tau_j$ -degree  $\delta_1$  and  $\delta_2$ , respectively, corresponding to the interpolation data  $\{(\lambda_i, \phi_i); i = 1, \dots, j\}$ .*

*Let  $\tau_{j \rightarrow J} := \delta_1 - \delta_2$ . Let  $B_{j \rightarrow J}(x)$  be a  $\tau_{j \rightarrow J}$ -reduced basis matrix corresponding to the interpolation data  $\{(\lambda_i, \phi_i B_j(\lambda_j)); i = j + 1, \dots, J\}$ .*

*Then  $B_J(x) := B_j(x)B_{j \rightarrow J}(x)$  is a  $\tau_J$ -reduced basis matrix corresponding to the interpolation data  $\{(\lambda_i, \phi_i); i = 1, \dots, J\}$ .*

*Proof.* For the proof, see [20]. □

When we apply this theorem with  $\lambda_j = \omega_j \in \mathfrak{U}_{2n}$  as interpolation points, we obtain a superfast algorithm in  $\mathcal{O}(n \log^2 n)$  to compute  $B(x)$ . See [20] for more details.

## 5. CONCLUSION

In this paper, we re-investigate the solution of a Toeplitz system  $Tu = g$  from a new point of view, by correlating the solution of such a problem with generators of the syzygy module  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  associated to the Toeplitz matrix  $T$ . We show that  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  is free of rank 2 and that it has a  $n$ -basis. We show that finding a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  is equivalent to computing the Gohberg-Semencul decomposition of  $T^{-1}$ , and we reduce the solution of  $Tu = g$  to an Euclidean division. We give two superfast algorithms computing a  $n$ -basis of  $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$  and a superfast algorithm to obtain the solution from this  $n$ -basis.

A perspective of this work is to generalize the approach to two-level Toeplitz systems or to Toeplitz-block-Toeplitz matrices and to correlate the basis computation of a multivariate syzygy module to “Gohberg-Semencul” decompositions for Toeplitz-block-Toeplitz matrices.

## REFERENCES

- [1] D. Bini and V. Y. Pan. *Polynomial and matrix computations. Vol. 1: Fundamental Algorithms*. Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994.
- [2] R. Bitmead and B. Anderson. Asymptotically fast solution of Toeplitz and related systems of equations. *Linear Algebra and Its Applications*, 34:103–116, 1980.
- [3] R. Brent, F. Gustavson, and D. Yun. Fast solution of Toeplitz systems of equations and computation of Padé approximants. *J. Algorithms*, 1:259–295, 1980.
- [4] D. Cox, J. Little, and D. O’Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.
- [5] P. Fuhrmann. *A polynomial approach to linear algebra*. Springer-Verlag, 1996.
- [6] I. Gohberg and N. Krupnik. A formula for the inversion of finite-section Toeplitz matrices. *Matem. Issled.*, 7(2):272–284, 1972. (In Russian).
- [7] I. Gohberg and A. Semencul. On the inversion of finite Toeplitz matrices and their continuous analogues. *Math. Issled.*, 2:201–233, 1972. (In Russian).
- [8] G. Heinig and K. Rost. *Algebraic methods for Toeplitz-like matrices and operators*, volume 13 of *Operator Theory: Advances and Applications*. Birkhäuser Verlag, Basel, 1984.
- [9] G. Heinig and K. Rost. *Algebraic methods for Toeplitz-like matrices and operators*. Akademie Verlag, Berlin, 1984. Also Birkhäuser Verlag, Basel.
- [10] T. Huckle. Computations with Gohberg-Semencul-type formulas for Toeplitz matrices. *Linear Algebra Appl.*, 273:169–198, 1998.
- [11] T. Kailath and J. Chun. Generalized Gohberg-Semencul formulas for matrix inversion. In H. Dym, S. Goldberg, M. Kaashoek, and P. Lancaster, editors, *The Gohberg anniversary collection, volume I: The Calgary conference and matrix theory papers*, volume 40 of *Operator Theory: Advances and Applications*, pages 231–246, Boston, 1989. Birkhäuser Verlag.
- [12] T. Kailath and A. H. Sayed. Displacement structure: theory and applications. *SIAM Rev.*, 37(3):297–386, 1995.
- [13] H. Khalil. *Structured and Toeplitz-block-Toeplitz matrices in numeric and symbolic computation*. Ph.D thesis. Institut Camille Jordan, Université Lyon 1, 2008. <http://tel.archives-ouvertes.fr/docs/00/30/69/87/PDF/these.pdf>.
- [14] G. Labahn and T. Shalom. Inversion of Toeplitz matrices with only two standard equations. *Linear Algebra Appl.*, 175:143–158, 1992.
- [15] B. Mourrain and V. Y. Pan. Multivariate polynomials, duality, and structured matrices. *J. Complexity*, 16(1):110–180, 2000.
- [16] V. Y. Pan. Nearly optimal computations with structured matrices. In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000)*, pages 953–962, New York, 2000. ACM.
- [17] V. Y. Pan. *Structured matrices and polynomials*. Birkhäuser Boston Inc., Boston, MA, 2001. Unified superfast algorithms.
- [18] W. Trench. An algorithm for the inversion of finite Toeplitz matrices. *J. SIAM*, 12:515–522, 1964.
- [19] E. Tyrtyshnikov. Fast algorithms for block Toeplitz matrices. *Sov. J. Numer. Math. Modelling*, 1(2):121–139, 1985.
- [20] M. Van Barel, G. Heinig, and P. Kravanja. A stabilized superfast solver for nonsymmetric Toeplitz systems. *SIAM J. Matrix Anal. Appl.*, 23(2):494–510, 2001.
- [21] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

HOUSSAM KHALIL, INSTITUT CAMILLE JORDAN, UNIVERSITÉ CLAUDE BERNARD LYON 1, 43 BOULEVARD DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE CEDEX FRANCE

*E-mail address:* `khalil@math.univ-lyon1.fr`

BERNARD MOURRAIN, INRIA, GALAAD TEAM, 2004 ROUTE DES LUCIOLES, BP 93, 06902 SOPHIA ANTIPOLIS CEDEX, FRANCE

*E-mail address:* `mourrain@sophia.inria.fr`

MICHELLE SCHATZMAN, INSTITUT CAMILLE JORDAN, UNIVERSITÉ CLAUDE BERNARD LYON 1, 43 BOULEVARD DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE CEDEX FRANCE

*E-mail address:* `schatz@math.univ-lyon1.fr`